DETAILED ACTION

1. Claims 1, 16-18, 21, 31, 37, 38, 40, 42, and 46-48 are amended in examiner's amendment.

2. Claims 1, 4, 6-9, 11-29, 31-35, 37-52, and 54-57 are allowed over art.

3. Claims 2-3, 5, 10, 30, 36, and 53 are cancelled by applicant.

EXAMINER'S AMENDMENT

4. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Richard Huffman on 9/26/2008.

The following claims are amended:

Claim 1: An apparatus for performing cryptographic operations, comprising:

a cryptographic instruction, received by a computing device microprocessor as part of an instruction flow executing on said ~~computing~~ device microprocessor, wherein said cryptographic instruction prescribes one of the cryptographic operations, be executed on a plurality of input text blocks, and wherein said cryptographic instruction also prescribes one of a plurality of block cipher modes to be employed in

accomplishing said one of the cryptographic operations, wherein said microprocessor comprises:

execution logic, operatively coupled to said cryptographic instruction, configured to execute said one of the cryptographic operations, wherein said one of the cryptographic operations, wherein said execution logic comprises:

a cryptography unit, configured execute a plurality of cryptographic rounds on each of said plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by a control word that is provided to said cryptography unit, and wherein said plurality of input text blocks are retrieved from memory, and wherein said plurality of output text blocks are stored to said memory;

indicating whether said one of the cryptographic operations has been interrupted by an interrupting event.

Claim 16: The apparatus as recited in claim 1, further comprising: block pointer logic, operatively coupled to said execution logic, configured to direct said computing device microprocessor to modify pointers to input and output data blocks in said memory to point to next input and output data blocks at the completion of said one of the cryptographic operations on a current input data block.

Claim 17: The apparatus as recited in claim 1, further comprising: block pointer logic, operatively coupled to said execution logic, configured to direct said computing device microprocessor to modify contents of a block counter register to indicate that said one of the cryptographic operations has been completed on a current input data block.

Claim 18: The apparatus as recited in claim 1, further comprising: block pointer logic, operatively coupled to said execution logic, configured to direct said computing device microprocessor to preserve or to generate and preserve data resulting from performance of said one of the cryptographic operations on a current block of data such that, upon return from said interrupting event, performance of said one of the cryptographic operations can continue with a following block of data.

Claim 21: The apparatus as recited in claim 1, wherein said cryptographic instruction implicitly references a plurality of registers within said ~~computing device~~ microprocessor.

Claim 31: The apparatus for performing cryptographic operations, comprising:

a cryptography unit within a device microprocessor, configured to execute one of the cryptographic operations responsive to receipt of a cryptographic instruction within an instruction flow that prescribes said one of the cryptographic operations, and wherein said cryptographic instruction also specifies one of a plurality of block cipher modes to be employed when performing said one of the cryptographic operations, and wherein said cryptography unit is configured execute a plurality of cryptographic rounds on each of said plurality of input text blocks to generate a corresponding each of a plurality of output data blocks, and wherein said plurality of input data blocks are retrieved from memory, and wherein said plurality of output data blocks are retrieved from memory; and

block pointer logic, operatively coupled to said cryptography unit, configured to direct said device microprocessor to modify pointers to said plurality of input and output

data blocks in memory to point to next input and output data blocks at the completion of said one of the cryptographic operations on a current input data blocks; and

a bit within a register in said microprocessor, operatively coupled to said cryptography unit, configured to indicate that execution of said one of the cryptographic operations has been interrupted by an interrupting event.

Claim 37: The apparatus as recited in claim 31, block pointer logic is configured to direct said device microprocessor to modify contents of a block counter register to indicate that said one of the cryptographic operations has been completed on a current input data block.

Claim 38: The apparatus as recited in claim 31, wherein said block pointer logic is configured to direct said device microprocessor to preserve or to generate and preserve data resulting from performance of said one of the cryptographic operations on a current block of data such that, upon return from said interrupting event, performance of said one of the cryptographic operations can continue with a following block of data.

Claim 40: A method for performing cryptographic operations in a device microprocessor, the method comprising:

fetching a cryptographic instruction from memory, wherein said cryptographic instruction prescribes one of the cryptographic operations along with one of a plurality of block cipher modes to be employed when performing the one or the cryptographic operations;

retrieving a plurality of input data blocks from memory;

via execution logic within the microprocessor, employing one of a plurality of block cipher modes to be and executing the one of the cryptographic operations on the plurality of input of data blocks to generate a corresponding plurality of output data blocks, wherein said executing is performed responsive to said fetching;

storing the corresponding plurality of output data blocks to the memory; and

indicating whether an interrupting event has occurred during said executing.

Claim 42: The method as recited in claim 41, wherein said indicating comprises modifying the state of a bit in a register within the device microprocessor.

Claim 46: The method as recited in claim 40, further comprising: directing the ~~device~~ microprocessor to modify pointers to said plurality of input and output data blocks in memory to point to next input and output data blocks at the completion of the one of the cryptographic operations on a current input data block.

Claim 47: The method as recited in claim 40, further comprising: directing the ~~device~~ microprocessor to modify contents of a block counter register to indicate that the one of the cryptographic operations has been completed on a current input data block.

Claim 48: The method as recited in claim 40, further comprising:

directing the device microprocessor to preserve or to generate and preserve data resulting from performance of the one of the cryptographic operations on a current block of data such that, upon return from the interrupting event, performance of the one of the cryptographic operations can continue with a following block of data.

Information Disclosure Statement

5. The information disclosure statement (IDS) submitted on 8/19/08; 9/4/08; 9/22/08 was filed after the mailing date of the Non-Final Rejection on 11/08/2008. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Allowable Subject Matter

6. The following is an examiner's statement of reasons for allowance:

The amendment made for claims 1, 4, 6-9, 11-29, 31-35, 37-52, and 54-57 in applicant's response on 5/29/2008 have overcome the non-final rejection mailed on 1/11/2008. A further search and examination concludes that prior art including the Hashimoto and Murantani combination does not teach or suggest the current claimed invention. Therefore, places 1, 4, 6-9, 11-29, 31-35, 37-52, and 54-57 in condition for allowance.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Leynna T. Truvan whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/L. T. T./
Examiner, Art Unit 2135
/KimYen Vu/
Supervisory Patent Examiner, Art Unit 2135